



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/679,879	10/06/2003	Hidema Tanaka	43521-0900	3840
21611	7590	02/20/2007	EXAMINER	
SNELL & WILMER LLP (OC) 600 ANTON BOULEVARD SUITE 1400 COSTA MESA, CA 92626			MORAN, RANDAL D	
			ART UNIT	PAPER NUMBER
2135				
SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE		
3 MONTHS	02/20/2007	PAPER		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>
	10/679,879	TANAKA ET AL.
	Examiner Randal D. Moran	Art Unit 2135

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

1)  Responsive to communication(s) filed on 06 October 2003.

2a)  This action is FINAL.                            2b)  This action is non-final.

3)  Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## **Disposition of Claims**

4)  Claim(s) 1-15 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.

5)  Claim(s) \_\_\_\_\_ is/are allowed.

6)  Claim(s) 1-15 is/are rejected.

7)  Claim(s) \_\_\_\_\_ is/are objected to.

8)  Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

9)  The specification is objected to by the Examiner.

10)  The drawing(s) filed on 06 October 2003 is/are: a)  accepted or b)  objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)  The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a)  All    b)  Some \* c)  None of:  
1.  Certified copies of the priority documents have been received.  
2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3.  Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1)  Notice of References Cited (PTO-892)  
2)  Notice of Draftsperson's Patent Drawing Review (PTO-948)  
3)  Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date *1/12/2004 and 1/23/2004*.  
4)  Interview Summary (PTO-413)  
Paper No(s)/Mail Date. *\_\_\_\_\_*.  
5)  Notice of Informal Patent Application  
6)  Other: *\_\_\_\_\_*.

## DETAILED ACTION

1. Claims 1-15 are pending in this application.
2. The IDS filed on 1/23/2004 has been considered by the examiner. The IDS filed on 1/23/2004 has different inventors and content from the instant application but has been considered.

### *Claim Objections*

3. The following claims are objected to for lack of antecedent basis.
  - Considering **Claims 1, 5, 7, 8, and 10**- line 10 recites the limitation, “the fixed parts.”
  - Considering **Claim 2**- line 12 recites the limitation, “the fixed parts.”
  - Considering **Claim 3**- line 14 recites the limitation, “the fixed parts.”
  - Considering **Claims 4 and 6**- line 9 recites the limitation, “the fixed parts.”
  - Considering **Claims 9 and 11**- line 11 recites the limitation, “the fixed parts.”
  - Considering **Claims 12, 13, 14, and 15**- line 13 recites the limitation, “the fixed parts.”

***Claim Rejections - 35 USC § 112***

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. **Claims 1-15** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

- Considering **Claims 1-15**, “counting the inputted plaintext having a value of the fixed part included in a set of values of the fixed parts at every set of the values of the fixed parts formed of one or a plurality of the values of the fixed parts, and storing it as a separate count” is vague and indefinite. It is unclear what counting the inputted plaintext means. It is also unclear what is meant by the value of the fixed part. The claim only contains a bit string and a fixed part. Therefore, the set of values of the fixed parts is unclear since there is only one fixed part. The fixed parts formed of 1 or a plurality of the values of the fixed parts is unclear. From the claim, there is only 1 count being made, therefore, it is unclear what storing it as a separate count means.
- Considering **Claims 5, 9, and 12, ¶ 7**, “cipher information required for setting the encryption algorithm executed by the encryption apparatus main body and counter part setting information required for setting information corresponding to the encryption algorithm for the fixed part

and the set of the values of the fixed parts and used by the counter part based on the indication signal" is unclear. Setting information required for setting information is unclear and needs to be explained. The set of values of the fixed parts is unclear since there is only one fixed part.

***Claim Rejections - 35 USC § 103***

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. **Claims 1, 2, 4, 6-8, 10, and 11** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Matyas, Jr. et al. (US 5,978,124)**, hereafter "Matyas," in view of **Lynn et al. (US 5,444,781)**, hereafter "Lynn".

7. Considering **Claim 1**, Matyas discloses a particular plaintext detector for detecting whether plaintext to be inputted into a predetermined encryption algorithm satisfies a predetermined condition (col. 4- lines 19-23), the particular plaintext detector comprising: a receiving part for receiving the plaintext (Fig. 1- item 100); a counter part for separating a predetermined part from a bit string forming the plaintext into a fixed part and a remaining part into a variable part

(Fig. 5), counting the inputted plaintext having a value of the fixed part included in a set of values of the fixed parts at every set of the values of the fixed parts formed of 1 or a plurality of the values of the fixed parts, and storing it as a separate count (Fig. 5- item 503-505, col. 4- lines 31-55).

Matyas does not disclose a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number.

Lynn does disclose a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number (Fig. 5, col. 5- lines 63-68, col. 6- lines 1-10).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Matyas by outputting a detection signal when the count exceeds a predetermined vale as taught by Lynn for the benefit of enabling the variability of the overall security of the transmitter and receiver by providing a selection of the number of times each temporal sequence is used in the encoding of the data (Lynn- col. 6- lines 22-26).

8. Considering **Claim 2**, Matyas discloses a particular plaintext detector for detecting whether plaintext to be inputted into a block encryption algorithm satisfies a predetermined condition (col. 4- lines 19-23), the block encryption algorithm receiving and stirring plaintext with a key step by step to perform encryption and outputting ciphertext (Fig. 1), the particular plaintext detector comprising: a receiving part for receiving the plaintext (Fig. 1- item 100); a

counter part for separating a predetermined part from a bit string forming the plaintext into a fixed part and a remaining part into a variable part (Fig. 5), counting the inputted plaintext having a value of the fixed part included in a set of values of the fixed parts at every set of the values of the fixed parts formed of 1 or a plurality of the values of the fixed parts, and storing it as a separate count (Fig. 5- item 503-505, col. 4- lines 31-55).

Matyas does not disclose a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number.

Lynn does disclose a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number (Fig. 5, col. 5- lines 63-68, col. 6- lines 1-10).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Matyas by outputting a detection signal when the count exceeds a predetermined vale as taught by Lynn for the benefit of enabling the variability of the overall security of the transmitter and receiver by providing a selection of the number of times each temporal sequence is used in the encoding of the data (Lynn- col. 6- lines 22-26).

9. Considering **Claim 4**, Matyas discloses a filter apparatus for limiting output of ciphertext from an encryption algorithm that receives plaintext to output ciphertext (Fig. 1, col. 3- lines 33-43), the filter apparatus comprising: a receiving part for receiving the plaintext (Fig. 1- item 100); a counter part for separating a

predetermined part from a bit string forming the plaintext into a fixed part and a remaining part into a variable part (Fig. 5), counting the inputted plaintext having a value of the fixed part included in a set of values of the fixed parts at every set of the values of the fixed parts formed of 1 or a plurality of the values of the fixed parts, and storing it as a separate count (Fig. 5- item 503-505, col. 4- lines 31-55).

Matyas does not disclose a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number.

Lynn does disclose a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number (Fig. 5, col. 5- lines 63-68, col. 6- lines 1-10).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Matyas by outputting a detection signal when the count exceeds a predetermined vale as taught by Lynn for the benefit of enabling the variability of the overall security of the transmitter and receiver by providing a selection of the number of times each temporal sequence is used in the encoding of the data (Lynn- col. 6- lines 22-26).

The combination of Maytas and Lynn discloses a filter apparatus main body for outputting the plaintext when a detection signal is not outputted from the detecting part (Lynn- Fig. 5, col. 5- lines 63-68, col. 6- lines 1-10), and for holding output of the plaintext until it receives a process restart signal for instructing

restart of outputting the plaintext when the detection signal is outputted (Maytas- col. 8- lines 2-10, Lynn- Fig. 2).

10. Considering **Claim 6**, Matyas discloses an encryption apparatus for executing an encryption algorithm that receives plaintext to calculate ciphertext with a key (Fig. 1, col. 3- lines 33-43), the encryption apparatus comprising: a receiving part for receiving the plaintext; (Fig. 1- item 100); a counter part for separating a predetermined part from a bit string forming the plaintext into a fixed part and a remaining part into a variable part (Fig. 5), counting the inputted plaintext having a value of the fixed part included in a set of values of the fixed parts at every set of the values of the fixed parts formed of 1 or a plurality of the values of the fixed parts, and storing it as a separate count (Fig. 5- item 503-505, col. 4- lines 31- 55).

Matyas does not disclose a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number.

Lynn does disclose a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number (Fig. 5, col. 5- lines 63-68, col. 6- lines 1-10).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Matyas by outputting a detection signal when the count exceeds a predetermined value as taught by Lynn for the benefit of enabling the variability of the overall security of the transmitter and

receiver by providing a selection of the number of times each temporal sequence is used in the encoding of the data (Lynn- col. 6- lines 22-26).

The combination of Matyas and Lynn discloses an encryption apparatus main body for updating the key used for encryption when a detection signal is outputted from the detecting part (Lynn- Fig. 5- item 65).

11. Considering **Claim 7**, Matyas discloses a ciphertext storing apparatus for executing an encryption algorithm that receives plaintext to calculate ciphertext with a key (Fig. 1, col. 3- lines 33-43), and storing the ciphertext (Fig. 6- item 150), the ciphertext storing apparatus comprising: a receiving part for receiving the plaintext (Fig. 1- item 100); a counter part for separating a predetermined part from a bit string forming the plaintext into a fixed part and a remaining part into a variable part (Fig. 5), counting the inputted plaintext having a value of the fixed part included in a set of values of the fixed parts at every set of the values of the fixed parts formed of 1 or a plurality of the values of the fixed parts, and storing it as a separate count (Fig. 5- item 503-505, col. 4- lines 31-55).

Matyas does not disclose a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number; a ciphertext storing part allowed to store ciphertext; and a ciphertext storing apparatus main body for updating the key used for encryption when a detection signal is outputted from the detecting part, and for storing partial plaintext being a part of the plaintext, the ciphertext, and key reference information allowing

reference of the key having been used for encryption in the ciphertext storing part.

Lynn does disclose a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number (Fig. 5, col. 5-lines 63-68, col. 6- lines 1-10); a ciphertext storing part allowed to store ciphertext (Fig. 4a- items 39,41,43, and 60); and a ciphertext storing apparatus main body for updating the key used for encryption when a detection signal is outputted from the detecting part (Fig. 5- item 65), and for storing partial plaintext being a part of the plaintext, the ciphertext, and key reference information allowing reference of the key having been used for encryption in the ciphertext storing part (Fig. 4a, Fig. 5- item 65).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Matyas by outputting a detection signal updating the key when the count exceeds a predetermined value and storing the necessary information as taught by Lynn for the benefit of enabling the variability of the overall security of the transmitter and receiver by providing a selection of the number of times each temporal sequence is used in the encoding of the data (Lynn- col. 6- lines 22-26).

12. Considering **Claims 8 and 10**, are rejected for the same reasons as claims 4 and 6 stated above.

13. Considering **Claim 11**, is rejected for the same reasons as claims 6 and 7 stated above.

Matyas discloses allowing reference of the key having been used for encryption in the ciphertext storing part (Fig. 5- item 502).

14. **Claims 3, 14, and 15** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Matyas and Lynn** in view of **Kasumi Specification. Specification of the 3GPP Confidentiality and Integrity Algorithms. Version 1.0, 23 December 1999. pg. 8-17**, hereafter "KASUMI."

15. Considering **Claim 3**, Matyas discloses the particular plaintext detector comprising: a receiving part for receiving the plaintext (Fig. 1- item 100); a counter part for separating 17th to 32nd bits of the plaintext from the plaintext into a fixed part and first to 16th bits and 33rd to 64th bits thereof into a variable part (Fig. 5, col. 6- lines 16-39), counting the inputted plaintext having a value of the fixed part included in a set of values of the fixed parts at every set of the values of the fixed parts formed of 1 or a plurality of the values of the fixed parts, and storing it as a separate count (Fig. 5- item 503-505, col. 4- lines 31-55). Matyas does not disclose a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number.

Lynn does disclose a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number (Fig. 5, col. 5-lines 63-68, col. 6-lines 1-10).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Matyas by outputting a detection signal when the count exceeds a predetermined vale as taught by Lynn for the benefit of enabling the variability of the overall security of the transmitter and receiver by providing a selection of the number of times each temporal sequence is used in the encoding of the data (Lynn- col. 6-lines 22-26).

The combination of Maytas and Lynn does not explicitly disclose a particular plaintext detector for detecting whether plaintext to be inputted into a KASUMI type encryption algorithm having a stirring step satisfies a predetermined condition, the KASUMI type encryption algorithm equal to KASUMI which is a block encryption algorithm that receives plaintext, has a plurality of stirring steps for stir with a key, and performs encryption step by step to output ciphertext. KASUMI does disclose a particular plaintext detector for detecting whether plaintext to be inputted into a KASUMI type encryption algorithm having a stirring step satisfies a predetermined condition, the KASUMI type encryption algorithm equal to KASUMI which is a block encryption algorithm that receives plaintext, has a plurality of stirring steps for stir with a key, and performs encryption step by step to output ciphertext (p. 8, Section 2.1- Introduction, p.10, Section 3-KASUMI Operation).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Matyas and Lynn by detecting whether plaintext is to be inputted into a KASUMI type encryption algorithm and performs encryption step as taught by KASUMI for the benefit of using an encryption algorithm that will increase the strength of the algorithm and is a well known standard in the art.

16. Considering **Claim 14**, is rejected for the same reasons as claims 3 and 6 stated above.
17. Considering **Claim 15**, is rejected for the same reasons as claims 3 and 7 stated above.
18. **Claims 5, 9, and 12** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Matyas and Lynn** in view of **Marchant (US 6,094,486)**.
19. Considering **Claim 5**, Matyas discloses the encryption apparatus comprising: a receiving part for receiving the plaintext (Fig. 1- item 100); a counter part for separating a predetermined part from a bit string forming the plaintext into a fixed part and a remaining part into a variable part (Fig. 5), counting the inputted plaintext having a value of the fixed part included in a set of values of the fixed parts at every set of the values of the fixed parts formed of 1 or a plurality of the

values of the fixed parts, and storing it as a separate count (Fig. 5- item 503-505, col. 4- lines 31-55).

Maytas does not disclose a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number.

Lynn does disclose a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number (Fig. 5, col. 5- lines 63-68, col. 6- lines 1-10).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Matyas by outputting a detection signal when the count exceeds a predetermined vale as taught by Lynn for the benefit of enabling the variability of the overall security of the transmitter and receiver by providing a selection of the number of times each temporal sequence is used in the encoding of the data (Lynn- col. 6- lines 22-26).

The combination of Matyas and Lynn discloses an encryption apparatus main body for performing the encryption algorithm for encryption when a detection signal is not outputted from the detecting part (Lynn- Fig. 5, col. 5- lines 63-68, col. 6- lines 1-10), and for holding output of the plaintext when the detection signal is outputted (Maytas- col. 8- lines 2-10, Lynn- Fig. 2).

The combination of Matyas and Lynn does not disclose an encryption apparatus for executing an encryption algorithm that receives plaintext to output ciphertext in which the encryption algorithm is changeable; an indication signal receiving part for receiving an indication signal for indicating an encryption algorithm for

new use; and a setting part for outputting cipher setting information required for setting the encryption algorithm executed by the encryption apparatus main body and counter part setting information required for setting information corresponding to the encryption algorithm for the fixed part and the set of the values of the fixed parts and used by the counter part based on the indication signal, wherein the encryption apparatus main body and the counter part perform the settings based on the cipher setting information and the counter part setting information.

Marchant does disclose an encryption apparatus for executing an encryption algorithm that receives plaintext to output ciphertext in which the encryption algorithm is changeable (Fig. 7- item 456 and 458, col. 2- lines 12-17); an indication signal receiving part for receiving an indication signal for indicating an encryption algorithm for new use (Fig. 7- item 456); and a setting part for outputting cipher setting information required for setting the encryption algorithm executed by the encryption apparatus main body and counter part setting information required for setting information corresponding to the encryption algorithm for the fixed part and the set of the values of the fixed parts and used by the counter part based on the indication signal (col. 10- lines 59-67, col. 11- lines 1-9), wherein the encryption apparatus main body and the counter part perform the settings based on the cipher setting information and the counter part setting (Fig. 4- item 202 and 204, col. 2- lines 12-17).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Matyas and Lynn by using a system that has the ability to change the encryption used for each string and being able to set it to respond to certain conditions as taught by Marchant for the benefit of using a random choice of encryption algorithms on a randomly chosen length of a string results in a code that is nearly impossible to break (Marchant- col. 3- lines 27-33).

20. Considering **Claim 9**, is rejected for the same reasons as claims 4 and 5 stated above.
21. Considering **Claim 12**, is rejected for the same reasons as claims 3 and 4 stated above.
22. **Claim 13** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Matyas, Lynn, KASUMI, and Marchant**.
23. Considering **Claim 13**, is rejected for the same reasons as claims 3, 4, and 5 stated above.

***Conclusion***

24. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- US 2003/0182435 – plaintext passed through a filter.
- US 5,768,276 – using different encryption algorithms.
- US 5,958,073 – detection of invalid plaintext entered.
- US 6,775,769 – plaintext filter.

25. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Randal D. Moran whose telephone number is 571-270-1255. The examiner can normally be reached on M-F: 7:00 - 4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Randal D. Moran

RDM  
2/15/07



KIM VU  
USPTO PATENT EXAMINER  
TECHNOLOGY CENTER 2100